REMOVAL OF DATA FROM DECOMMISSIONED STORAGE DEVICES

Status:	**Active Policy**
Effective Date:	July 5, 2006 through June 30, 2008
Revised Date:	N/A
Approved By:	J. Stephen Fletcher, CIO
Authority:	*UCA §63F-1-206; Governor's Executive Order: Directing the Chief Information Officer to Develop and Implement Policy Promoting Security of State Information and Information Systems*

1.1 PURPOSE

To establish a policy and procedure detailing the criteria by which qualified Department of Technology Services (DTS) employees in authorized positions clear, erase, and remove all data and software from personal computers, file servers, and disk subsystems prior to decommissioning.

1.1.1 Background

External audits have identified the existence of data on hard drives in equipment designated to be surplused. This policy is intended to reduce the potential for unauthorized recovery of data from decommissioned equipment.

1.1.2 Scope

This policy and procedure applies to all personal computers, file servers, or electronic storage equipment supported, maintained, or administered by the DTS and the employees with responsibilities related to these devices. This policy also addresses the disposition of outdated or surplused equipment and the removal of all data and software from resident hard drives.

1.1.3 Exceptions

Agencies excluded under the provisions of *§63F-1-102 (7) et seq.,* are not included under the provisions of this policy.

1.2 DEFINITIONS

Removal of State of Utah Data
Removal of data from hard drives is the process of removing sensitive and/or confidential programs or data files on computer hard drives in a manner that gives assurance that the information cannot be recovered by keyboard or laboratory efforts.

Overwriting
The process of erasing, or “wiping,” the contents of an electronic file or disk space. Overwriting of data means replacing previously stored data on a drive with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable. It is impossible to restore data on storage media that has been properly “wiped.”

1.3 POLICY

All personal computers, hard drives, file servers, or disk subsystems, supported, maintained, owned, or administered by DTS shall have all residing State of Utah data and software removed prior to the equipment's decommission. Any evidence of ownership or use of the equipment must also be removed to ensure that no data of any type is left on the equipment.

All decommissioned equipment addressed in this policy must follow a uniform and consistent method for the removal of data and software from the hard drive or storage media. The process will be performed for all departments and divisions whose desktop equipment is serviced by DTS.

1.4 PROCEDURE

There are two acceptable methods to be used for data storage devices and hard drive data destruction:

1.4.1 Overwriting

1.4.1.1 Overwriting is the approved method for removal of agency data from hard disk storage media.

1.4.1.2 Software used by DTS personnel for data wiping must be endorsed by the State Chief Information Security Officer (CISO). The CISO shall also maintain records of all personnel that are certified and trained to decommission storage devices.

1.4.1.3 DTS requires three wipes minimum, overwriting each character with a character, its compliment, then a random character.

1.4.1.3.1 Additional overwriting methods may be employed via various CISO endorsed software packages which allow for a massive number of passes to virtually ensure absolute data sanitization.

1.4.2 Physical Destruction

1.4.2.1 The physical destruction of hard disk media is a process whereby the physical storage media is rendered useless and inaccessible. This can be performed by any number of methods, but the end result is that the individual “platters” of the storage media are left in numerous fragments.

1.4.2.2 Disposition and tracking of the remaining and unusable hard disk storage media will be performed systematically with the proper involvement of tracking documentation, and the training of appropriate DTS staff. The process for destruction and disposition of fragments of storage devices must be endorsed by the department's Chief Operations Officer and CISO.

1.4.3 Removal of Data and Software

All decommissioned equipment addressed in this policy must follow a uniform and consistent method for the removal of data and software from the hard drive or storage media. The process will be performed for all agencies whose desktop equipment is decommissioned by DTS.

1.4.3.1 Identify equipment to be removed from inventory and prepared for decommissioning. This will be performed in conjunction with the agency being serviced by DTS.

1.4.3.3 Trained DTS staff will use CISO approved standard methods to “wipe” data storage media and at a minimum perform a “Level Three” wipe process on all equipment. Once a “wipe” is completed no data (including an operating system) will reside on the device.

1.4.3.4 Equipment will be marked with a DTS tag indicating that data has been cleared from the storage media.

1.4.3.5 In conjunction with requirements of the Division of Surplus Property, an SP1 Form will be completed, and the tag number will be recorded.

1.4.3.6 An audit process, as defined and initiated by the CISO, will verify that the disposition of the decommissioned equipment is performed accurately.

1.4.3.7 If the storage media is inaccessible through electronic means, the media may be destroyed and rendered useless per the guidelines referenced in 1.4.2.1

1.5 APPENDICES

- Department of Defense (DoD) 5220.22-M guidelines
- Memorandum of Understanding between DTS and DAS for Surplus Property

---

DOCUMENT HISTORY

Originator:	Dave Fletcher
Next Review:	May 15, 2008
Reviewed Date:	N/A
Reviewed By:	N/A